Check Pointin haittaohjelmakatsaus 7/2018

Pankkitroijalaiset hyödyntävät turistien piittaamattomuutta – hyökkäyskuvio tuttu viime kesältä

Tietoturvayhtiö Check Pointin maailmanlaajuinen uhkaindeksi kertoo, että kesäkuussa troijalaiset kapusivat mukaan haittaohjelmatilaston kymmenen kärkeen. Kryptolouhijat pysyivät kuitenkin edelleen listan huipulla.

ESPOO —16. heinäkuuta 2018. Pankkitroijalaisten vaikutus on kasvanut maailmanlaajuisesti 50 prosenttia viimeisen neljän kuukauden aikana. Check Pointin haittaohjelmatilaston kymmenen kärjessä on nyt kaksi troijalaiskantaa.

Kesäkuussa Dorkbot, arkaluontoisia tietoja varastava ja palvelunestohyökkäyksiä käynnistävä pankkitroijalainen, vaikutti 7 prosenttiin maailman yrityksistä. Samalla se nousi Check Pointin haittaohjelmatilastossa kahdeksannelta sijalta peräti kolmanneksi. Myös Suomen listalla Dorkbot nousi hieman matalammalla vaikutusprosentilla viidenneksi, kun edellisessä kuussa se ei ollut edes haittaohjelmien kymmenen kärjessä.

Kesäkuussa näki päivänvalon myös Emotet-nimellä tunnettu pankkitroijalainen. Ohjelma varastaa uhrien pankkitilien käyttöoikeudet samalla, kun se käyttää tartunnan saaneita laitteita uusien tartuntojen levittämiseen. Emotet-ohjelman muunnos on yleistynyt nopeasti viimeisen kahden kuukauden aikana – huhtikuun indeksissä se oli sijalla 50, kun viimeisimmässä listauksessa se on sijalla 11.

– Havaitsimme kesällä 2017 samankaltaisen aggressiivisen hyökkäyskuvion, jossa verkkorikolliset käyttivät pankkitroijalaisia. Tämä viittaa siihen, että hakkerit yrittävät kenties käyttää hyväkseen turisteja, jotka kiinnittävät lomalla vähemmän huomiota tietoturvakäytäntöihin. Moni saattaa käyttää verkkopankkia julkisesti jaetuilla laitteilla tai huonosti suojatuilla verkkoyhteyksillä. Hakkerit ovatkin sinnikkäitä ja viekkaita yrityksissään varastaa rahaa, kertoo Check Pointin tietoturvatutkijoiden ryhmää vetävä **Maya Horowitz**.

Horowitz muistuttaa, että valtava enemmistö verkkorikollisuudesta on taloudellisesti motivoituneiden hakkereiden tekemää.

– He käyttävät laajaa työkaluvalikoimaansa yksinkertaisesti löytääkseen tavan, jolla tehdä kustannustehokkaimmin nopeaa voittoa. Jotta pankkitroijalaisia ja muun tyyppisiä hyökkäyksiä voidaan torjua, on elintärkeää, että yrityksillä on monitasoinen kyberturvallisuusstrategia vakiintuneilta haittaohjelmilta sekä uusilta uhilta suojautumiseen.

Haittaohjelmat kesäkuussa Top 5, Suomi:

1. **Coinhive** - Kryptolouhija, joka on suunniteltu louhimaan Moneroa käyttäjän tietämättä, kun tämä vierailee verkkosivulla.
2. **Nivdort** - Troijalainen, joka leviää sähköpostiliitteiden tai haitallisten verkkosivujen avulla.
3. **Roughted** - Laajan skaalan haittamainosohjelma, joka voi tarjota reitin myös kiristysohjelmille.
4. **Cryptoloot** - Kryptovaluuttalouhija, Coinhiven kilpailija**.**
5. **Dorkbot –** Viestikeskustelujen kautta leviävä pankkitroijalainen, joka varastaa arkaluontoisia tietoja ja käynnistää palvelunestohyökkäyksiä.

Haittaohjelmat kesäkuussa Top 3, maailma:
**Nuoli osoittaa muutoksen listasijoituksessa edelliseen kuukauteen verrattuna.*

1. ↔ **Coinhive** – Kryptolouhija, joka on suunniteltu louhimaan Moneroa käyttäjän tietämättä, kun tämä vierailee verkkosivulla.
2. ↔ **Cryptoloot** - Kryptolouhija, joka käyttää uhrin koneen prosessoritehoa kryptovaluutan louhimiseen.
3. ↑**Dorkbot** - Viestikeskusteluihin pohjautuva pankkitroijalainen, joka varastaa arkaluontoisia tietoja ja käynnistää palvelunestohyökkäyksiä.

Mobiililaitteiden haittaohjelmat kesäkuussa Top 3, maailma:

1. **Triada** - Android-laitteissa leviävä ohjelma, joka tarjoaa käyttöoikeuksia muille puhelimen haittaohjelmille ja auttaa niitä sulautumaan osaksi käyttöjärjestelmää.
2. **Lokibot** - Android-laitteissa leviävä pankkitroijalainen, joka voi myös muuntua kiristysohjelmaksi lukiten puhelimen.
3. **The Truth Spy** - Applen ja Android-puhelinten vakoiluohjelma, joka mahdollistaa käynnissä olevien toimintojen seuraamisen.

Check Pointin tutkijat analysoivat myös yleisimpiä haavoittuvuuksia. Kesäkuussa haavoittuvin oli 40 prosentin maailmanlaajuisella vaikutuksella CVE-2017-7269. Sitä seurasi CVE-2017-10271, jota oli hyödynnetty 35 prosentissa organisaatioista, ja kolmantena listalla oli SQL-injektiohaavoittuvuus 15 prosentilla.

Kuukausittain laadittava haittaohjelmatilasto perustuu Check Pointin ThreatCloudin™ tietoihin. Se on maailman laajin verkosto, joka kerää tietoja kyberhyökkäyksistä ja näyttää ne reaaliaikaisesti kartalla. Verkosto tunnistaa päivittäin miljoonia haittaohjelmatyyppejä analysoidessaan yli 250 miljoonasta verkko-osoitteesta saamiaan tietoja.

Täydellinen Top 10 -haittaohjelmalista löytyy Check Pointin blogista osoitteesta:
https://blog.checkpoint.com/2018/07/05/junes-most-wanted-malware-banking-trojans-crypto-mining/

Check Pointin uhkientorjuntaresurssit ovat saatavilla osoitteesta http://www.checkpoint.com/threat-prevention-resources/index.html

Lisätiedot ja haastattelupyynnöt:

Maajohtaja Robert Lindqvist, Check Point Software Technologies, robertl@checkpoint.com, p. 050 368 4912

OSG Viestintä, Matleena Merta, matleena.merta@osg.fi, p. 0447366060

Seuraa Check Pointia:
Twitter: http://www.twitter.com/checkpointsw
Facebook: https://www.facebook.com/checkpointsoftware
Blog: http://blog.checkpoint.com
YouTube: http://www.youtube.com/user/CPGlobal
LinkedIn: https://www.linkedin.com/company/check-point-software-technologies

Check Point Software Technologies Ltd.
Check Point Software Technologies Ltd. (www.checkpoint.com) on maailman suurin tietoverkkojen kyberturvallisuuteen keskittynyt yhtiö. Se tarjoaa alan johtavia ratkaisuja ja suojelee asiakkaitaan kyberhyökkäyksiltä vertaansa vaille olevalla haittaohjelmien, kiristysohjelmien ja muiden tietoturvan uhkien

kiinnijäämisprosentilla. Check Pointin kattava tietoturva-arkkitehtuuri suojaa niin yrityksen verkot, pilvipalvelut kuin mobiililaitteetkin, ja myös sen hallintajärjestelmä on kattava ja intuitiivinen. Check Point huolehtii yli 100 000 yrityksen ja yhteisön tietoturvatarpeista organisaation koosta riippumatta.

